What Is Claimed Is:

1. A method for managing public keys through a server that stores associations between public keys and email addresses, comprising:

receiving a first message from a client at the server, the first message containing a request for approval of a client public key along with the client public key;

sending a second message from the server to the client, the second message containing a request for identity confirmation that includes the client public key; and

if a third message is received from the client at the server containing an affirmative response to the request for identity confirmation, storing an association between a client email address and the client public key in a database, so that other clients can look up the client public key in the database.

2. The method of claim 1, further comprising:

receiving a communication from a second client at the server, the communication including the client email address;

performing a lookup in the database based on the client email address to determine if the client email address is associated with the client public key;

if the lookup indicates that the client email address is associated with the client public key, sending a key identifier for the client public key from the server to the client, wherein the key identifier allows the client to determine whether the client possesses the client public key.

3. The method of claim 1,

wherein the request for approval includes key reconstitution information that allows the client to decrypt to an encrypted client private key at the client if the client forgets a passphrase for decrypting the encrypted client private key; and

wherein the method further comprises storing the key reconstitution information in the database.

4. The method of claim 1, further comprising:

decrypting the request for approval at the server using a server private key, the request for approval having been encrypted with a corresponding server public key by the client; and

using the client public key to verify that the request for approval is signed by a corresponding client private key.

5. The method of claim 1, wherein prior to sending the second message, the method further comprises:

determining if the database already contains a prior client public key associated with the client email address; and

if the database already contains the prior client public key, including the prior client public key in the request for identity confirmation sent to the client in the second message, so that the client can indicate that the server should replace the prior client public key with the client public key.

6. The method of claim 1, further comprising:

receiving a request at the server to remove the client public key from the database;

if the request is signed with a corresponding client private key, removing the client public key from the database.

7. The method of claim 1, wherein the database contains at most one key for each email address.

8. The method of claim 1, wherein the database contains at most one email address for each key.

9. The method of claim 1, further comprising:

periodically sending a verification request from the server to the client email address asking if the client public key remains valid; and

if an affirmative response to the verification request is not received, removing the client public key from the database.

10. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for managing public keys through a server that stores associations between public keys and email addresses, the method comprising:

receiving a first message from a client at the server, the first message containing a request for approval of a client public key along with the client public key;

sending a second message from the server to the client, the second message containing a request for identity confirmation that includes the client public key; and

if a third message is received from the client at the server containing an affirmative response to the request for identity confirmation, storing an association between a client email address and the client public key in a database, so that other clients can look up the client public key in the database.

11. The computer-readable storage medium of claim 10, wherein the method further comprises:

receiving a communication from a second client at the server, the communication including the client email address;

performing a lookup in the database based on the client email address to determine if the client email address is associated with the client public key;

if the lookup indicates that the client email address is associated with the client public key, sending a key identifier for the client public key from the server to the client, wherein the key identifier allows the client to determine whether the client possesses the client public key.

12. The computer-readable storage medium of claim 10,

wherein the request for approval includes key reconstitution information that allows the client to decrypt to an encrypted client private key at the client if the client forgets a passphrase for decrypting the encrypted client private key; and

wherein the method further comprises storing the key reconstitution information in the database.

13. The computer-readable storage medium of claim 10, wherein the method further comprises:

decrypting the request for approval at the server using a server private key, the request for approval having been encrypted with a corresponding server public key by the client; and

using the client public key to verify that the request for approval is signed by a corresponding client private key.

14. The computer-readable storage medium of claim 10, wherein prior to sending the second message, the method further comprises:

determining if the database already contains a prior client public key associated with the client email address; and

if the database already contains the prior client public key, including the prior client public key in the request for identity confirmation sent to the client in the second message, so that the client can indicate that the server should replace the prior client public key with the client public key.

15. The computer-readable storage medium of claim 10, wherein the method further comprises:

receiving a request at the server to remove the client public key from the database;

if the request is signed with a corresponding client private key, removing the client public key from the database.

16. The computer-readable storage medium of claim 10, wherein the database contains at most one key for each email address.

17. The computer-readable storage medium of claim 10, wherein the database contains at most one email address for each key.

18. The computer-readable storage medium of claim 10, wherein the method further comprises:

periodically sending a verification request from the server to the client email address asking if the client public key remains valid; and

if an affirmative response to the verification request is not received, removing the client public key from the database.

19. An apparatus that facilitates managing public keys through a server that stores associations between public keys and email addresses, the apparatus comprising:

a receiving mechanism at the server that is configured to receive a first message from a client, the first message containing a request for approval of a client public key along with the client public key;

a sending mechanism that is configured to send a second message to the client, the second message containing a request for identity confirmation that includes the client public key; and

a database located at the server;

a storing mechanism coupled to the database, wherein if the receiving mechanism receives a third message from the client containing an affirmative response to the request for identity confirmation, the storing mechanism is configured to store an association between a client email address and the client public key in a database, so that other clients can look up the client public key in the database.

20. The apparatus of claim 19, further comprising a key lookup mechanism that is configured to:

receive a communication from a second client at the server, the communication including the client email address;

perform a lookup in the database based on the client email address to determine if the client email address is associated with the client public key; and to

send a key identifier for the client public key from the server to the client, if the lookup indicates that the client email address is associated with the client public key, wherein the key identifier allows the client to determine whether the client possesses the client public key.

21. The apparatus of claim 19,

wherein the request for approval includes key reconstitution information that allows the client to decrypt to an encrypted client private key at the client if the client forgets a passphrase for decrypting the encrypted client private key; and

wherein the storing mechanism is additionally configured to store the key reconstitution information in the database.

22. The apparatus of claim 19, further comprising:

a decryption mechanism that is configured to decrypt the request for approval at the server using a server private key, the request for approval having been encrypted with a corresponding server public key by the client; and

a verification mechanism that is configured to use the client public key to verify that the request for approval is signed by a corresponding client private key.

23. The apparatus of claim 19, further comprising a lookup mechanism that is configured to determine if the database already contains a prior client public key associated with the client email address;

wherein if the database already contains the prior client public key, the sending mechanism is additionally configured to include the prior client public key in the request for identity confirmation sent to the client, so that the client can indicate that the server should replace the prior client public key with the client public key.

24. The apparatus of claim 19, further comprising a key removal mechanism that is configured to:

receive a request at the server to remove the client public key from the database; and to

remove the client public key from the database, if the request is signed with a corresponding client private key.

25. The apparatus of claim 19, wherein the database contains at most one key for each email address.

26. The apparatus of claim 19, wherein the database contains at most one email address for each key.

27. The apparatus of claim 19, further comprising a key removal mechanism that is configured to:

send a verification request from the server to the client email address asking if the client public key remains valid; and to

remove the client public key from the database, if an affirmative response to the verification request is not received.